POLYCOM

Release Note
Video Border Proxy
Version 9.1.5.1

Contents

Introduction

This document describes the enhancements and fixes provided by the Polycom Video Border Proxy (VBP) VoIP Operating System (VOS), version 9.1.5.1. It includes all modifications made since VBP VOS version 7.2.2

This VBP release support's all legacy VBP H.323/H.460 scenario's and adds support for the new Polycom VC2 endpoint experience to the VBP-ST platform.

Software requirements for Interoperability

- CMA 4000/5000 server – 4.01.02 or higher (see note)
- CMA Desktop – 4.1.1 or higher
- HDX – 2.5.0.5 or higher

Note: The following issues, which may impact VBP functionality exist in CMA 4.01.02. These issues are addressed in CMA version 4.01.04

- Duplicate Aliases – When a CMAD or HDX in VC2 mode moves from an internal CMA connection to an external VBP Access Proxy connection you might experience a scenario where the endpoint cannot connect to the CMA Server. An HDX endpoint is likely in this state if it displays an indicator stating that the gatekeeper service is down. A CMAD client is likely in this state if cannot progress beyond the "signing into the media server" message. In some cases, gracefully logging out of the internal location and waiting at least 10 minutes before an external login can reduce the chances of experiencing this issue.

- Dual Redundancy – When deploying 2 VBP's and 2 CMA server's for what is called "Dual Redundancy" if the MASTER CMA server fails, this forces the BACKUP CMA server to have control of all services, it is possible when this CMA failover happens, this CMA server may NOT send responses from the VIP (virtual IP) causing messages to be sent from the physical IP, the VBP is expecting messages to come from the VIP and will not be forwarded to the remote client. When deploying "Single Redundancy" 2 VBP's and 1 CMA server, If the MASTER VBP fails, the BACKUP VBP will take over and function as expected.

Known Issues

- In VOS 9.1.5.1 the Polycom VBP-E series does not support the Access Proxy feature, although the feature is present in the GUI. VBP-E series platforms will support this feature in a future release. Access Proxy feature support is fully functional in the VBP-ST series.
- It has been found in the field that 2Wire DSL termination routers have issues with H.323/H.460 protocols – to date, there is a currently a "single" video endpoint work around, 2Wire configuration parameters can be set on this router to support 1 H.323/H.460 endpoint. Please contact Polycom technical services if you are attempting to use CMA Desktop, HDX or other H.460 compatible video endpoints behind this device.

Installation Recommendation

Platform	Upgrade Recommendation	Comment
All VBP Platforms	Recommended	This release has features and bug fixes which relate to issues that were found in the field for the VBP series appliance and are recommended. This release includes an SSH daemon security update introduced in VOS 9.1.3. This release includes a VRRP behavior change that was introduced in 8.9. This change will not affect currently configured VRRP systems.

NAT routers tested

Manufacture	**Model –HW version**	**SW version**	**Multiple H.460 endpoints**	**Issues noticed**
Netgear	WGR614-v9	1.2.2NA	Yes	none
Linksys	WRT54GL-v1.1	4.30.11	Yes	none
Dlink	WBR-1310-B1	2.00	No *	Router tends to reboot occasionally
Linksys	WRT54G2-v1	1.0.01	Yes	none
Belkin	F5D9231-4-v1	1.00.01	Yes	none

* Dlink WBR-1310 can support only 1 H.460 endpoint, the first endpoint that registers is the only endpoint that will work, even if this 1st endpoint has been powered down. This router creates "H.323" connection tracking at the MAC layer, the only way to clear this is to reboot the router. After a reboot you can now register a new H.460 device.

Supported Platforms

VOS version 9.1.5.1 is released for the following VBP Series products:

- 200EW-E
- 4300-E
- 4350-E
- 4350EW-E
- 5300-E and ST
- 5300LF-E and ST
- 6400-E and ST
- 6400LF-E and ST
- 6400lf2-E and ST

New Features introduced in VOS 9.1.5.1

- None

Fixes and Enhancements in VOS 9.1.5.1

- Bug 4074: Log rotation fix for iptables logging - log rotation capability has also been added to Access Proxy, the system will now have 8, 250K ap-iptables.log files located in /var/log that track the dynamic "add" or "delete" firewall rules for authenticated VC2 based endpoints. This file also tracks VC2 endpoints that have become unavailable that indicates they have been "deleted".
    - ap-iptables.log
    - ap-iptables.log.1
    - ap-iptables.log.2
    - ap-iptables.log.3
    - ap-iptables.log.4
    - ap-iptables.log.5
    - ap-iptables.log.5
    - ap-iptables.log.6
    - ap-iptables.log.7

- Bug 4075: Fixed accessproxyrc startup problem with multi cores, 6400, 6400LF, 6400LF2

New Features introduced in VOS 9.1.5

- Copied key/cert to /usr/local/ssl/certs
- Access Proxy
    - Added support for HDX. Changed handling of the incoming authentication message from the HDX client.
- Allow LAN side E/P's to dial ANNEX O If an incoming call used an AnnexO dialing string where the IP address was the address of the system itself, we would not forward the call. Now we strip of the IP address from the alias if it is matching the address of the system itself, and completes the call using the alias part of the AnnexO string.

Fixes and Enhancements in VOS 9.1.5

- Bug 2298: Annex-O LAN->LAN calls are GK routed.
- Bug 3883: VBP incorrectly assigning RTP ports We now attempt to match the RTP forwarding entries according to the signaled session IDs so that the forward and reverse stream gets the same port number.
- Bug 3857: Access Proxy - Enable Logging. Default Access Proxy.conf file has been copied to /etc/default/ for reference. Additional enhancements to the log messages to provide before information.
- Bug 3858: Access Proxy - Added Log Level support. Access proxy can now print out logs of varying levels by modifying /etc/config/Access Proxy.conf. Update LOG_LEVEL with either LVL_INF, LVL_DBG, LVL_DAT.

- Bug 3867: Access Proxy - HTTPS access to the system on alternate port. Firewall rules in config_ep_fw.sh and config_em_fw.sh have been updated. Text/Warnings has also been updated on the Firewall page, HTTPS Certificate page and the Access Proxy page.
- Bug 3873: Access Proxy - VRRP Support. Access proxy will start via /etc/Access Proxyrc if VRRP is enabled and is in MASTER state. Access Proxy will self-terminate if the state changes to BACKUP.
- Bug 3873: Access Proxy - VRRP Support. Modified config_vrrp.sh to insert the appropriate allow iptables rules when the system is running in VBP-ST mode.
- Bug 3859: In Embedded Gatekeeper mode, not all the aliases are display this limitation has been removed.
- Message of the Day" configured or not; a longer than 8 characters password will now be rejected.
- Bug 3929: bandwidth tracking problem for h.460 nat'd endpoint initiated calls, this is a result of the fix for bug 2217 and is now resolved.

New Features introduced in VOS 9.1.4

- Access Proxy Secure ALG functionality: In secure mode, the Access Proxy will have the following functionality:
    - Automatic AdapterProbe message response.
    - Automatic UpdateCheck message response with xml: <appUpdate>NONE</appUpdate>
    - Default iptables rule for blocking ALL traffic to XMPP (5222) and LDAP (389) ports.
    - Authentication message validation.
    - Dynamic addition / deletion of iptables access rule per user based on authentication 200OK response from CMA Server.
    - Addition of internal client list for tracking client access.
    - Log out handling → removes client from internal ap-client.list, iptables access rule removal.
    - Heartbeat handling → updates the session time for client in internal list.
    - Session time expiration handling (60 minutes) → Removes expired clients from the list and iptables.
    - Access Proxy now runs in Secure mode as a default.
    - Debug log rotation capability has also been added to Access Proxy, the system will now have 8, 250K accessproxy.log files located in /var/log note: debug is NOT enabled by default and must be enabled in the /etc/config/accessproxy.conf file please contact Polycom technical services for the correct instructions
        - accessproxy.log
        - accessproxy.log.1
        - accessproxy.log.2
        - accessproxy.log.3
        - accessproxy.log.4
        - accessproxy.log.5
        - accessproxy.log.6
        - accessproxy.log.7

- Bug 4383 Added the option "Supports Additive RRQ" in the RCF response from our embedded GK. This should allow our downstream VBP-ST to register more than 25 endpoints.

Fixes and Enhancements in VOS 9.1.4

- Bug 3483: Added the option "Supports Additive RRQ" in the RCF response from our embedded GK. This should allow our downstream VBP-ST to register more than 25 endpoints.
- Bug 3053: Inconsistent GUI password login length when you have "HTTP Short System Message" The behavior is now the same whether there is a "Short System Authorization
- Bug 2542: "?" is not allowed as the first character in the password It is now possible to use "?" in GUI passwords, as the first character or any other character.

New Features introduced in VOS 9.1.3

- Access Proxy functionality was added to the VBP-ST system which can be accessed through the menu. In addition, you will also see the "Access Proxy" configuration on the VBP-E series appliances, the feature is not fully supported on the E series system in this version, please do not attempt to configure this feature in this version. The E series Access Proxy feature will be supported in a future Polycom VBP VOS version.
- Security update: Upgrading openssh-4.0p1 to openssh-5.1p1

Fixes and Enhancements in VOS 9.1.3

- Enhancement: Polycom private / public security keys were added to ST and E models.
- Bug 3426: When HTTPS management is enabled, an attempt to add an HTTPS proxy server will now result in a message instructing the user to disable the HTTPS management from the Firewall page. If after the addition of the HTTPS proxy server, the HTTPS management is enabled, a message stating that HTTPS proxy and HTTPS management will be using different ports will be displayed.
- Bug 3293: NAT GUI: leading and/or trailing spaces in the port fields cause SNAT rule to not be applied in iptables. Leading and trailing spaces in the port fields caused parsing problems in the scripts. When saving the NAT rule, spaces are now stripped out of the rule before it is saved.
- Bug 3257: Re-enable MPPE support in kernel for PPTP server.

New Features introduced in VOS 8.11.1

- 6400LF2 platform was introduced in VOS 8.11.1

Fixes and Enhancements in VOS 8.11.1

- Bug 0899: "Erase" button did not function on 5300LF. The button now works the same as on all the other devices which is as follows:
    - Pressed once: Nothing happens.
    - Pressed twice: The CLI password is reset.
    - Pressed three times: The device is set to the factory defaults
- Bug 3191: Default gateway was not being set on the subscriber eth0 interface of "ST" devices.
- Bug: 2929: Removed Test UA from GUI.

- Bug: 3546: VBP system reports a 200AW hardware type but actual hardware is a 200EW, the issue is now resolved.
- Bug: 3012: ALG crashes with a LifeSize Express endpoint places call, the issue is now resolved.

New Features introduce in VOS 8.9.1

- Support for VBP 200EW and VBP 4350W was added.
- DHCP options 67 (boot file), 150, 151, 159, & 160 were added to DHCP GUI page for better interoperability with Polycom phones.
- H.323 activity log is now written to a separate log file with a maximum of 25 entries and with newer entries on top of the file. This prevents the H.323 activity log from being overwritten by other syslog activity.
- Added more feedback and controls to the upgrade page. Added a checkbox that displays the output from the upgrade command. Added the platform name to the upgrade page. Added a checkbox to enable/disable the FTP server ping check. Improved error feedback when an upgrade fails.
- Message of the Day (MOTD) is now displayed on VBP-ST systems.
- Feature/Bugfix: Improved reliability of VRRP. Numerous fixes: + Re-applied patches for multiple race-conditions. + Modified VRRP to only advertise on LAN link. WAN link status is still monitored but only the LAN has advertisements. This should prevent ping-ponging of state due to conflicting advertisements on different links. + Re-enabled revertive mode and made it user configurable. + Modified keepalived's script notification to be synchronous to fix a state issue race condition + Added VRRP state check in ALG causing ALG to self-terminate if we're in backup mode to prevent a situation where ALG is running even though we're in backup mode. + Increased default advertisement interval to 3 seconds to prevent VRRP state from going from FAULT to BACKUP to MASTER when recovering from a fault.

Fixes and Enhancements in VOS 8.9.1

- Enhancement: Capability was added to function in a router only mode.
- Bug 2832: PPoE was not coming up on WAN after the execution of “ewn load” command. This problem is now fixed.
- Bug 2558: Multicast gatekeeper requests were not being answered by VBP. This problem is now fixed.
- Bug 2733: LAN to LAN call using prefix routing was failing. This problem is now fixed.
- Bug 2560: VBP was not forwarding LRQ on the WAN side. This problem is now fixed.
- Bug fix: ALG was failing if a call came on a shared call appearance phone. This problem is now fixed.
- Bug 2806: All references to V2IU were converted to VBP in 200 and 4350 series.
- Bug 2810: SIP UA and GW were removed from 200 series GUI. Test UA, however, has not been removed since no analog ports are needed to run Test UA.
- Bug 2808: (200 Platform) A video call would terminate by itself after a certain amount of time.
- Bug 2582: One way audio was observed on certain H.460 endpoints. This problem is now fixed.
- Bug 2267: Q.931 was not being blocked when H.323 was enabled. TCP port 1720 is now blocked by firewall when H.323 is enabled which blocks Q.931 traffic.

- Bug: H.323 - Transparent LRQ in LAN GK mode was not working.
- Bug: ALG was failing while receiving an incoming WAN call in LAN side gatekeeper mode. This problem is now fixed.
- Bug 1288: H.460.18 traversal was not working when used with a RadVision GK and a Tandberg endpoint.
- Bug: ALG was failing when endpoints were registering with multiple aliases containing the same string.
- Bug: SIP stale RTP deletion feature was incorrectly deleting active H.323 calls which would cause ALG to malfunction.
- Bug 2217 LAN side prefix routing is counting bandwidth, the issue is now resolved.
- Bug 2496: Removed the Route GUI page and renamed the VoIP subnet routing page to Route. VoIP subnet routes are not limited to the ALG so the two pages were redundant.
- Bug 140: ADSL-PPPoE is displayed in the GUI for the following platforms 5300, 5300LF, 6400, 6400LF, 6400LF2, this is not a support WAN type for these platforms. Removed ADSL-PPPoE network option from the 5300, 5300LF, 6400, 6400LF, and 6400LF2.
- Bug 1848: 6400 and 6400LF does not have HTTPS as an option in the GUI. Added support for HTTPS on 6400, 6400LF. Added of the certificate link and the HTTPS firewall check box for these platforms.

Upgrade Instructions

This version of software is available on the Polycom Support FTP site: ftp.support.polycom.com

It is recommended you reboot the Polycom VBP Series appliance prior to doing the upgrade. This will ensure there is enough dynamic memory available to handle the upgrade process.

When you update your software all services will be unavailable for several minutes. It is therefore advised that upgrades be performed during a maintenance window when VoIP traffic can be interrupted.

Upgrade procedure

1) Use a web browser to connect to the **VBP** appliance.
2) Click on the **Upgrade firmware** link. Use the page defaults.
3) Press **Submit**.
4) Follow the progress of the upgrade using the "refresh the upgrade status" link.
5) When the Write process begins, please heed the warning:

WARNING!!! Do not change the configuration or power off the device until the write is 100 percent complete. The device may become unusable if the write is interrupted.

6) The system will automatically restart after the new image has been loaded. After the upgrade process has completed, check that the new version number is displayed on the main System page.

Obtaining Further Assistance

Please contact the Polycom Technical Services for assistance.